

REPORT SAMPLE

報告書サンプル

Webセキュリティ 診断報告書

診断で見つかった問題と、その影響、
修正方法をまとめた報告書の記載例です。



WEB SECURITY ASSESSMENT

想定プロジェクト

会員向けWebサービス / 検証環境

TARGET

demo.example.invalid

DOCUMENT

WSL-SAMPLE-20261020 / v2.2

このサンプルについて

指摘内容や通信例は、説明用に作成した架空のものです。
実際の診断やテストは行っていません。実在する顧客の情報は
使用していません。

診断結果の要約

指摘は3件です。修正を勧める順番と理由を以下にまとめました。詳細は6〜8ページをご覧ください。

03

指摘例

中：1件 / 低：2件

04

影響箇所の例

重複を除いたエンドポイント数

未実施

実施状態

この資料は架空のサンプル

所見（記載例）

先にセッションCookieへHttpOnlyを設定してください。エラー応答から内部情報を除く修正も必要です。CSPは読み込みを遮断する影響があるため、動作確認後の適用を勧めます。

対応順序 / 判断の理由

01

F-01 / セッション保護

中

認証に使うCookieのため、用途と発行箇所を確認してから修正します。

02

F-03 / エラー表示

低

応答から内部情報を除き、詳細は運用担当者向けのログに残します。

03

F-02 / CSP導入

低

必要な読み込み元を洗い出し、監視モードで影響を確認してから適用します。

目次

対象と評価 03

指摘一覧 05

詳細と証跡 06

修正計画 09

QAチェック 10

重要度の基準は4ページ、修正計画は9ページを参照してください。

対象と実施条件

会員向けWebサービスを対象とした記載例です。

対象ホスト	demo.example.invalid (架空)
環境 / 権限	検証環境1つ / 一般会員1ロールを想定
対象規模	8エンドポイントの記載例 / 1ホスト
診断期間 / 実施者	未実施 / 担当者欄は実案件で記載
実施条件	対象の許諾、時間帯、負荷、停止条件を事前に合意

対象エンドポイント一覧

ID	METHOD / PATH	機能	関連する指摘例
E-01	GET /login	ログイン画面	—
E-02	POST /login	ログイン処理	F-01
E-03	POST /logout	ログアウト処理	—
E-04	GET /account	会員ページ	F-02
E-05	GET /settings	設定画面	F-02
E-06	POST /settings	設定更新	—
E-07	GET /api/profile	プロフィール参照	—
E-08	GET /error-demo	検証用エラー画面	F-03

エンドポイントはHTTPメソッドと正規化したパスの組み合わせで数えます。関連欄が「—」の箇所は、このサンプルの指摘に対応していません。すべて未診断です。

03 / ASSESSMENT FRAMEWORK

重要度の基準と確認方法

重要度は、攻撃が成立する条件と想定される影響から判断します。

重要度の基準と指摘件数（例）

高

大きな影響があり、攻撃が成立する条件も現実的な問題。

速やかに対策を検討します。

0

中

利用条件や他の問題との組み合わせで影響が増す問題。

用途と成立条件を確認し、対策を計画します。

1

低

防御の補強や限定的な情報露出に関する問題。

既存機能への影響を確認して修正します。

2

情報

判断材料や運用改善のための参考事項。

仕様や運用を確認して、対応の要否を決めます。

0

担当者による確認

01

対象を把握

到達範囲・認証を確認

→

02

内容を確認

応答と再現条件を確認

→

03

報告書を作成

重要度と修正案を記載

担当者が検出内容を確認し、再現確認済み、判断保留、誤検知に分類します。検出された件数と、報告する指摘件数は分けて記録します。

このサンプルの3件は架空例です。重要度は上記の基準による記載例とし、CVSSスコアは算出していません。

04 / FINDINGS REGISTER

指摘一覧

指摘ごとに証跡IDと修正後のテスト項目を記載しています。

F-01

重要度：中

セッションCookieのHttpOnly未設定

POST /login

EV-01 / 1箇所 / 詳細 p.06

QA-01～05

F-02

重要度：低

Content-Security-Policy (CSP) 未設定

GET /account, GET /settings

EV-02 / 2箇所 / 詳細 p.07

QA-06～08

F-03

重要度：低

詳細エラー情報の表示

GET /error-demo

EV-03 / 1箇所 / 詳細 p.08

QA-09～10

指摘ごとの記載内容

FINDING

確認した内容と影響



ACTION

修正方法



QA

操作手順と期待結果

集計では、原因と修正方法が同じ問題を1件として数えます。この例は指摘3件、影響箇所4件です。F-02は2箇所です同じ問題が起きる想定のため、1件にまとめています。

05 / FINDING DETAIL / F-01

セッションCookieのHttpOnly未設定

セッションCookieのHttpOnly属性がない想定例 / 重要度：中 / 実確認なし

E-02 / EV-01

POST /login

EV-01 / 応答抜粋の合成例 / 値は架空のプレースホルダー

```
HTTP/1.1 302 Found
Location: /account
Set-Cookie: session=[SAMPLE]; Path=/; Secure; SameSite=Lax
```

確認する手順

1. 検証用アカウントでログインし、Cookieを発行する応答を取得。
2. セッション用途のCookieを特定し、HttpOnly属性の有無を確認。
3. Cookieの用途とJavaScriptからの参照要否を開発担当者に確認。

想定される影響と成立条件

同じオリジンで不正なJavaScriptが実行される問題などが成立すると、Cookieを読み取られるおそれがあります。この例では、XSSの有無は確認していません。

修正方法

Cookieを発行する共通設定にHttpOnlyを追加してください。JavaScriptでCookieを読む処理がある場合は、その処理も修正対象です。ブラウザからサーバーへのCookie送信は続きます。

修正後の応答イメージ / 属性は実際の仕様に合わせて調整

```
Set-Cookie: session=[SAMPLE]; Path=/; Secure;
HttpOnly; SameSite=Lax
```

完了条件：HttpOnlyがあり、認証機能のテスト（QA-01～05）を満たす。

QA-01～05 → p.10 / 技術資料 R-01 → p.12

06 / FINDING DETAIL / F-02

Content-Security-Policy未設定

Content-Security-Policy (CSP) がない想定例 / 重要度 : 低 / 実確認なし

E-04, 05 / EV-02

GET /account, GET /settings

EV-02 / 応答: 文書を確認した場合の記載イメージ / 合成例

HTTP/1.1 200 OK

Content-Type: text/html; charset=utf-8

[Review] No CSP header or CSP meta policy in this example.

確認する手順

1. 各HTML応答のCSPヘッダーと、HTML内のmetaによる指定を確認。
2. CDNなどの配信経路による設定差と、既存の制御方針を確認。
3. 外部スクリプト、画像、API接続など、必要な読み込み元を整理。

想定される影響と成立条件

不正なスクリプト等の読み込みをCSPで制限できない状態です。CSPがないだけでXSSが成立するとは限りません。入力値の検証や出力時の処理も確認します。

修正方法

最初はReport-Onlyで、どの読み込みが違反になるかを確認してください。必要な読み込み元を絞り、主要画面や外部連携が動くことを確かめてから強制適用します。インライン処理にはnonceやhashの利用も検討します。

01 / 整理

読み込み元を棚卸し

02 / 監視

Report-Onlyで観測

03 / 適用

動作確認後に強制

完了条件 : 合意したポリシーが応答に適用され、主要機能に不要な遮断がない。

QA-06〜08 → p.10 / 技術資料 R-02 → p.12

07 / FINDING DETAIL / F-03

レスポンスへの詳細エラー出力

詳細なエラー情報を応答に含める想定例 / 重要度：低 / 実確認なし

E-08 / EV-03

GET /error-demo

EV-03 / エラー応答の合成例 / 実在するコード・内部パスではありません

```
HTTP/1.1 500 Internal Server Error
Content-Type: application/json

{"error":"SampleError",
 "trace":"at DemoAccountService (internal/example:42)"}

```

確認する手順

1. 許可された検証用のエラー操作で、エラー時の応答を確認。
2. 本文・ヘッダーに内部の処理名やスタックトレースがないか確認。
3. 通常画面、API、共通エラーハンドラーの設定差を確認。

想定される影響と成立条件

内部の処理名やファイル構成を、第三者に知られるおそれがあります。この例に認証情報や個人情報の漏えいは含めていません。実際の応答に含まれる情報と公開範囲を確認します。

修正方法

エラー応答には利用者向けの案内と問い合わせIDを返してください。内部の処理名やスタックトレースは、運用担当者だけが読めるログに残します。パスワードやトークンはログにも記録しません。

利用者：一般的な案内 + 問い合わせID

運用担当：必要な詳細を権限付きログで確認

完了条件：応答に内部詳細が出ず、運用担当がIDで事象を追跡できる。

QA-09～10 → p.10 / 技術資料 R-03 → p.12

修正計画

修正の担当者と完了条件を決めるための記載例です。

01

F-01 / セッションCookie

想定担当：バックエンド

Cookieの発行箇所と、JavaScriptで読み取る処理を調べる。HttpOnlyを追加し、ログインとログアウトを試す。

完了条件：HttpOnlyが付与され、QA-01～05を満たす。

02

F-03 / エラー表示

想定担当：バックエンドと運用

共通エラーハンドラーの応答から内部情報を除く。問い合わせIDで、運用担当者がログを探せるようにする。

完了条件：内部詳細が表示されず、QA-09～10を満たす。

03

F-02 / CSP

想定担当：フロントエンドと配信基盤

必要な読み込み元を一覧にする。Report-Onlyで違反を調べ、主要機能が動くことを確かめてから適用する。

完了条件：適用状況と主要機能を確認し、QA-06～08を満たす。

開発チケットの記載項目

指摘ID / 対象の設定・ファイル / 担当者 / 予定日 / 変更内容 / 確認したQA項目 / 修正後の証跡。期限は依存関係とリリース予定に合わせて決めます。

この例ではCookieの修正を先に勧めています。着手前に開発担当者が関連する処理を調べ、工数と期限を決めてください。

修正後の簡易テスト項目

指摘に関連する10項目です。実行前に、仕様と対象ブラウザに合わせて調整してください。

ID / 関連	操作・確認	期待結果	結果
01 / F-01	ログイン後のCookie属性を確認。	セッションCookieにHttpOnlyがある。	未実施
02 / F-01	正しい認証情報でログイン。	会員ページが表示される。	未実施
03 / F-01	誤ったパスワードでログイン。	認証できず、内部情報のない案内が表示される。	未実施
04 / F-01	ログイン後に画面移動・再読み込み。	仕様上の有効期間内はログイン状態を維持する。	未実施
05 / F-01	ログアウト後に会員ページへ再アクセス。	認証が必要になり、終了済みセッションで閲覧できない。	未実施
06 / F-02	各対象HTMLの応答とポリシーを確認。	合意したCSPが配信経路を含めて適用される。	未実施
07 / F-02	設定画面・画像・API連携を操作。	必要な読み込みや操作が遮断されずに完了する。	未実施
08 / F-02	検証環境で合意した禁止元の読み込みを確認。	強制適用時は対象の読み込みが遮断される。	未実施
09 / F-03	検証用エラーを画面・APIで発生させる。	応答に内部処理名・スタックトレースが出ない。	未実施
10 / F-03	問い合わせIDを使って運用ログを確認。	権限のある担当者が該当事象を追跡できる。	未実施

許諾を得た環境と検証用アカウントを使ってください。実行時には日付、担当者、ブラウザを記録し、各項目に結果と証跡を残します。失敗した項目は、関連する修正内容を確認します。

10 / VERIFICATION & HANDOFF

修正確認記録

指摘の再現確認と、関連機能のテスト結果を記入します。

修正確認の対象例：F-01

診断時と同じ環境でCookieの属性を確認し、修正前のEV-01と比較します。QA-01～05の結果も記録します。以下は記入前の様式です。

修正確認シート / 記入前の例

指摘ID / 対象	F-01 / E-02 / POST /login
修正内容	未記入（実施担当者が変更内容を記録）
変更識別子 / 確認日時	未記入 / 未実施
修正後の証跡ID	未採番（応答の比較用証跡を保管）
診断観点の判定	未実施：HttpOnlyの有無と適用範囲を確認
QA観点の結果	未実施：QA-01～05の実行結果を記録
残件 / 次の対応	未記入（判断保留事項と担当を記録）

判定ラベル

解消を確認

対象の指摘が再現しない

未解消

同じ条件で指摘が残る

判断保留

再確認の条件が揃わない

標準の修正確認は、同じ環境の重要度が高または中の指摘を最大5件まで、報告後30日以内に1回行います。この例ではF-01が対象です。F-02とF-03は、開発担当者が10ページの項目を使って確認します。

11 / REFERENCE & DOCUMENT CONTROL

参考資料と文書情報

指摘の内容や修正方法を確認する際の参照先です。

技術資料

R-01 / F-01

MDN: Set-Cookie

OPEN

HttpOnlyやSecureなど、Cookie属性の説明。

R-02 / F-02

MDN: Content Security Policy

OPEN

CSPの設定方法とReport-Onlyの使い方。

R-03 / F-03

OWASP: Error Handling Cheat Sheet

OPEN

エラー応答と内部ログに記録する内容の説明。

技術資料の確認日：2026年10月20日。カードを選択すると元資料を開きます。

用語

指摘ID / F-xx

修正すべき課題を追跡するための番号。

証跡ID / EV-xx

判断に使った応答や画面などを紐付ける番号。

QA項目 / QA-xx

修正後に確認する操作と期待結果。

重要度と対応順

重要度は問題の影響、対応順は修正作業を進める順序。

文書情報

Web診断ライト / 報告書サンプル v2.2

更新：2026年10月20日 / 指摘内容と証跡は架空

問い合わせ：tukkin0708@gmail.com